

GUTRIDE SAFIER LLP

Seth A. Safier (State Bar No. 197427)

seth@gutridesafier.com

Marie McCrary (State Bar No. 262670)

marie@gutridesafier.com

Todd Kennedy (State Bar No. 250267)

todd@gutridesafier.com

100 Pine Street, Suite 1250

San Francisco, California 94111

Telephone: (415) 639-9090

Facsimile: (415) 449-6469

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

Brandon Briskin, on behalf of
himself and those similarly situated,

Plaintiff,

v.

Shopify Inc. and Shopify (USA)
Inc.,

Defendants.

Case No. _____

Class Action Complaint

Jury Trial Demanded

1 Plaintiff Brandon Briskin brings this action on behalf of himself and all
2 others similarly situated against Shopify Inc. and Shopify (USA) Inc.
3 (collectively, “Shopify”). Plaintiff’s allegations against Shopify are based upon
4 information and belief and upon investigation of Plaintiff’s counsel, except for
5 allegations specifically pertaining to Plaintiff, which are based upon Plaintiff’s
6 personal knowledge.

7 **Introduction**

8 1. Shopify is an e-commerce platform that enables merchants to easily sell
9 products online. Many of Shopify’s customers are merchants who operate
10 websites and mobile applications, such as IABMFG. Shopify created software
11 code to enable merchants to integrate Shopify’s payment forms into their
12 applications. To that end, Shopify provides comprehensive documentation to its
13 merchant customers, describing how to integrate payment forms into their
14 websites and applications using the Shopify code, including how to omit Shopify
15 branding such that the form appears to the consumer to belong to the merchant’s
16 website.

17 2. In fact, despite the appearance to consumers that their payment
18 information is being sent to the merchant, it is intercepted by Shopify. When a
19 merchant integrates the Shopify software code into a website or mobile
20 application, consumers who desire to pay for a product or service are presented
21 with Shopify payment forms, which are created by Shopify. The payment forms
22 require the consumer to provide a variety of sensitive information, such as:

- 23 • name
- 24 • address
- 25 • telephone number
- 26

- email address
- complete credit card information, including cvc

3. Shopify also collects and indefinitely stores sensitive information about consumers using its payment form such as:

- The consumers' internet IP addresses;
- the brand and model of the consumer's computers or electronic devices;
- the identities of the consumer's browsers;
- the operating systems that the consumer's devices were using; and
- the item(s) purchased by the consumer from the merchants' websites.

4. Although consumers using merchants' websites and mobile applications reasonably expect that they are communicating directly with the merchant, Shopify's software code is designed to enable Shopify's computer network to intercept those communications and redirect them to Shopify's computer network. Shopify, however, designed its payment forms to omit all Shopify branding. Accordingly, the consumer has no idea that Shopify is involved in the transaction in any way, let alone that Shopify will be obtaining, storing, and evaluating the consumer's sensitive communications and information.

5. The Shopify code also surreptitiously installs tracking cookies on consumers' computers and mobile devices, which enable Shopify to identify a particular consumer and track his or her activities across its entire merchant network, enabling Shopify to gather even more sensitive data about the consumer including, without limitation, (i) the number of declined cards that the consumer has used with Shopify merchants; (ii) how long ago one of the consumer's cards was last declined; (iii) whether the consumer had ever disputed a previous

1 Shopify charge; (iv) whether any previous early fraud warnings were associated
2 with the consumer; (v) the percentage of transactions that were authorized for the
3 consumer over time; and (vi) the cards and other payment methods associated
4 with the consumer's IP address.

5 6. Shopify does not use consumers' private information simply for the
6 purposes of processing the payments in question. Instead, Shopify indefinitely
7 stores the information, correlates all payments from the consumer made across its
8 entire platform, and then—without informing the consumer—provides much of it
9 to its other merchants. For example, once a consumer has submitted a payment for
10 a purchase from IABMFG, any of Shopify's millions of other merchant customers
11 will then be able to access the consumer's private information pertaining to that
12 payment, as well as any other payment that Shopify processed for that consumer
13 in a profile for that consumer.

14 7. At no time does Shopify inform consumers who use its payment forms
15 on merchant websites that: (i) Shopify will intercept communications that
16 consumers believe are being sent exclusively to merchants; (ii) its software code
17 is causing their devices to connect to Shopify's computer servers; (iii) Shopify is
18 accessing consumers' data by placing tracking cookies on their devices; (iv) its
19 software code is rendering the payment forms that are displayed to consumers;
20 (v) the sensitive information in the payment forms will be sent to Shopify;
21 (vi) sensitive information not expressly inputted by the consumer—such as IP
22 address, operating system, geolocation data, and item(s) purchased—will also be
23 collected from the consumer by Shopify; (vii) Shopify will indefinitely store that
24 sensitive information; (viii) Shopify will use consumers' information to create
25 profiles of consumers, which could subsequently be communicated to other
26

1 merchants; (ix) Shopify will track consumers' behavior across over more than one
2 million websites; and (x) Shopify will make consumers' sensitive information
3 available to any of its millions of merchant customers who will accept payment—
4 or who have already accepted payment—from those consumers.

5 6 **Parties**

7 8. Plaintiff Brandon Briskin is, and was at all relevant times, an individual
8 and resident of California. Plaintiff currently resides in Madera, California.

9 9. Defendant Shopify Inc. is a Canadian company headquartered in
10 Ottawa, Canada with a domestic office in San Francisco, California.

11 10. Defendant Shopify (USA) Inc. is a Delaware company with its
12 principal place of business in Ottawa, Canada. Shopify (USA) Inc. is registered to
13 do business in California and has a domestic office in San Francisco, California.

14 11. Shopify Inc. and Shopify (USA) Inc. are referred to collectively herein
15 as “Shopify.”

16 **Jurisdiction and Venue**

17 12. This Court has subject matter jurisdiction over this action pursuant to
18 the Class Action Fairness Act, 28 U.S.C. Section 1332(d)(2)(A) because: (i) there
19 are 100 or more class members, and (ii) there is an aggregate amount in
20 controversy exceeding \$5,000,000, exclusive of interest and costs.

21 13. This Court has supplemental jurisdiction over any state law claims
22 pursuant to 28 U.S.C. Section 1367.

23 14. The injuries, damages and/or harm upon which this action is based
24 occurred or arose out of activities engaged in by Shopify within, affecting, and
25 emanating from the State of California. Shopify regularly conducts and/or solicits
26

1 business in, engages in other persistent courses of conduct in, and/or derives
2 substantial revenue from products provided to persons in the State of California.
3 Shopify has engaged, and continues to engage, in substantial and continuous
4 business practices in the State of California.

5 15. Venue is proper in this District pursuant to 28 U.S.C. Section
6 1391(b)(2) because a substantial part of the events or omissions giving rise to the
7 claims occurred in the state of California, including within this District.

8 16. Plaintiff accordingly alleges that jurisdiction and venue are proper in
9 this Court.

10 11 **Substantive Allegations**

12 **A. Shopify Surreptitiously Intercepts Consumers' Communications** 13 **and Collects their Private Information When They Make Online** 14 **Payments to Merchants.**

15 17. Shopify is an e-commerce platform that enables merchants to sell
16 products online. In June 2019, Shopify reported that it had more than 1,000,000
17 businesses in approximately 175 countries using its platform, with total gross
18 merchandise volume exceeding \$41 billion for calendar year 2018.¹ Using
19 Shopify's website, merchants provide Shopify with their product offerings, prices,
20 shipping options and other business preferences. Shopify hosts some of its
21 merchants' websites and creates all of the code necessary to implement the
22 product catalog and to accept payment. In addition, merchants who already own
23 websites can elect to embed certain Shopify assets, such as payment forms, into
24 their pre-existing websites. Regardless of the implementation, Shopify handles the

25 ¹ Shopify Announces Fourth-Quarter and Full Year 2018 Financial Results,
26 Businesswire.com, available at:
<https://www.businesswire.com/news/home/20190212005234/en/> (last accessed
August 2, 2021).

1 collection and validation of the consumer's payment information, as well as
2 processing the payment, through its relationships with third parties, such as Stripe.


3 18. To display payment forms to consumers, Shopify sends executable
4 javascript code to consumers' computers or mobile devices, which then execute
5 the code. Upon execution, the code loads and displays the payment forms to
6 consumers.

7 19. Shopify does not disclose to consumers its role in the transaction, let
8 alone that Shopify is sending code to consumers' devices to display the payment
9 forms. To the consumer, the website and payment forms appear to be generated
10 by the merchant itself. Thus, a consumer never knows that they have shared their
11 sensitive information, including sensitive financial information, to Shopify.

12 20. For example, consumers who order apparel or accessories on the
13 IABMFG website are presented with a cart page before proceeding to the
14 checkout page. The bottom of the cart page features a number of icons for various
15 forms of payment, including Visa, Mastercard and American Express. The
16 Shopify icon is presented alongside the credit card icons, making it appear to
17 consumers that Shopify is optional or a type of payment method the consumer
18 could choose akin to a credit card even though it is not.

19 21. Consumers who proceed with purchasing goods on the IABMFG
20 website are presented with the following payment form:
21
22
23
24
25
26

1 IAB|MFG.

2  Show order summary ▾ \$70.00

3

4 [Cart](#) > [Information](#) > [Shipping](#) > [Payment](#)

5 **Contact information** [Already have an account? Log in](#)

6

7 ☒ Keep me up to date on news and exclusive offers

8 **Shipping address**

9

10

11

12

13

14 ?

15 ☐ Save this information for next time

16 [Return to cart](#)

17 **Figure 1: IABMFG Checkout Page**

18 22. All of the input elements in the form (i.e., those corresponding to

19 “Email,” “First name,” “Last name,” “Address,” “Apartment, suite, etc.,” “City,”

20 “Country/Region,” “State,” “ZIP code,” and “Phone”) are generated by Shopify.²

21 To the user, however, it appears that the form and input elements are generated

22 and provided by IABMFG. Shopify does not cause its involvement in the

23 transaction to be displayed to the consumer alongside the payment form.

24

25 ² This is confirmed by the fact that the input elements are located in a <div>

26 tag having the class “edit_checkout”—a class that Shopify uses throughout its network of merchant websites.

23. Only a person with technical knowledge and special software tools could determine that the payment forms are generated by Shopify. As shown by the following screenshot from such a tool, the IABMFG checkout page above required the user's browser to load at least eight separate files—including four executable javascript files—from Shopify's computer network:

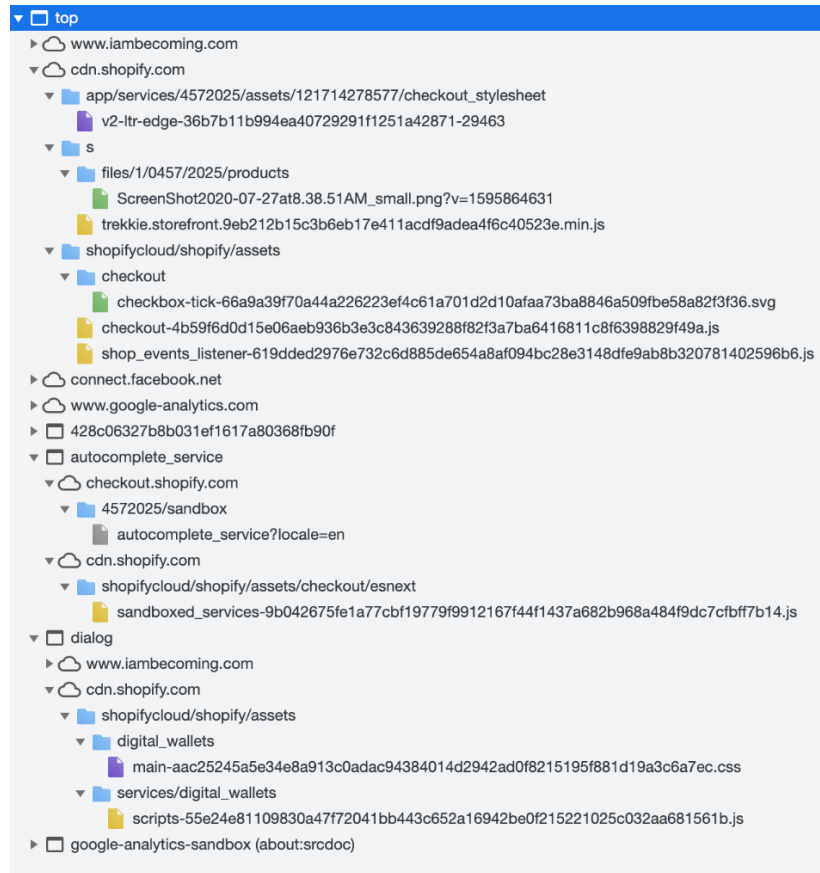


Figure 2: Assets loaded from Shopify during rendering of IABMFG checkout page

24. After submitting the shipping information form on the IABMFG website, the user is presented with a payment form:

Payment

All transactions are secure and encrypted.

☒ Credit card VISA AMEX and more...

Card number

Name on card

Expiration date (MM / YY) Security code

☐ VABILL Easy monthly payments VISA AMEX

[Pay now](#) [Return to shipping](#)

Billing address

Select the address that matches your card or payment method.

☒ Same as shipping address

☐ Use a different billing address

Figure 3: IABMFG Payment Form

25. Once again, the payment form—including the input elements—is generated by Shopify and sent to the user’s browser. To the user, however, it appears that the payment form is being generated by the IABMFG website. As is true of the shipping form, Shopify does not disclose its involvement in the transaction to the consumer.

26. When the user clicks the “Pay now” button, the Shopify-produced javascript code is executed on the user’s computer, causing the payment details to be collected from the form, and then sent directly to Shopify’s servers, at <https://deposit.us.shopifycs.com/sessions>. For example, the payload sent to that

address in a test transaction conducted on April 12, 2021, as seen through a special software tool, was as follows:

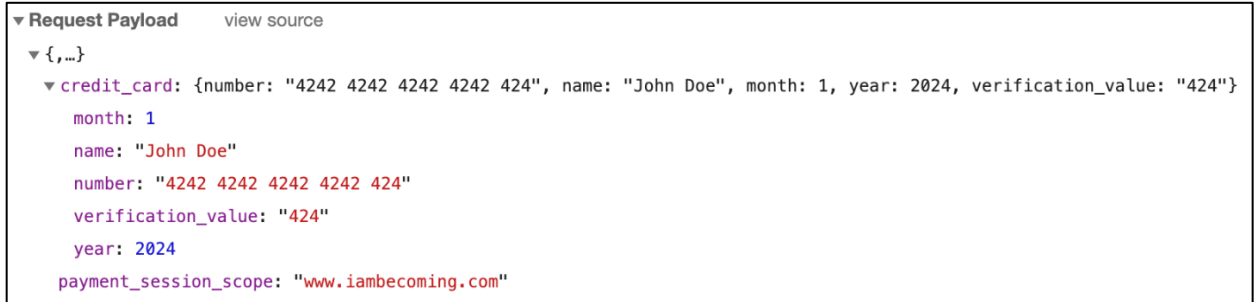


Figure 4: Request Payload to Shopify

27. As the figure above displays, the data sent directly to Shopify includes the user's name and sensitive payment information. This payload request, however, is just one of many requests that Shopify causes the user's browser to make to Shopify. Dozens of urls were also called by the user's browser upon clicking the "Pay now" button during the April 12 test transaction. None of these url calls are visible to the consumer.

28. When a consumer completes and submits the shipping and payment forms, it appears to the consumer that the information in the forms will be sent directly to the merchant. However, Shopify's software code, which has been installed on the user's computer without his or her consent, ensures that consumers' communications—including the private information in the forms—are intercepted and rerouted to Shopify's computer servers, including the servers that receive the requests listed above.

29. After the consumer has completed a purchase transaction, Shopify sends the user an order confirmation email. The email does not mention Shopify, let alone disclose to the consumer that Shopify has obtained and stored his or her

1 sensitive information and communications. Instead, it appears that it was sent by
2 the merchant. The “From” email address is identical to the merchant’s email.

3 30. The receipt email that Shopify sends to consumers contains a button
4 entitled “View your order.” Consumers who click the button are taken to the
5 merchant’s website and are shown a webpage that, although hosted and/or created
6 by Shopify, does not mention Shopify or disclose its involvement. Rather, to the
7 consumer, the page appears to have been created and hosted by the merchant.

8 31. Shopify’s involvement with the consumer’s private information does
9 not end when the transaction is completed. To the contrary, Shopify’s
10 involvement has only begun. Now that Shopify has the consumer’s information,
11 Shopify will track the consumer’s behavior across its vast merchant network. To
12 achieve this, Shopify installs a tracking cookie on the user’s browser. This cookie
13 may be installed when the user visits the payment page, or any other page of the
14 merchant’s website.

15 32. For example, merely viewing a single item on the IABMFG website
16 (the IABMFG Flex High Waisted Capri Pants, at
17 <https://www.iambecoming.com/collections/iab-flex-high-waisted-capri>) caused at
18 least six Shopify tracking cookies to be installed on the browser:

- 19
- 20 • `_shopify_sa_p`
 - 21 • `_shopify_sa_t`
 - 22 • `_shopify_s`
 - 23 • `_shopify_y`
 - 24 • `_shopify_fs`
 - 25 • `_shopify_country`
 - 26

1 33. Although the contents of Shopify cookies are encrypted, such that one
2 cannot view their contents without the decryption key, it is known that these
3 cookies are used to track consumers, their devices, and their behavior. The cookie
4 “_shopify_y,” for example, contains a unique code that uniquely identifies the
5 consumer’s device, so that Shopify can track the consumer’s behavior across its
6 vast merchant network. Further, it is known that Shopify collects and stores at
7 least the following information about customers of merchants such as IABMFG:

- 8 • name;
- 9 • email address;
- 10 • company;
- 11 • shipping address;
- 12 • billing address;
- 13 • phone number;
- 14 • amount spent;
- 15 • IP address;
- 16 • user agent (i.e., the user’s browser); and
- 17 • geolocation data.

18 34. Shopify makes *all* of this information available to its merchants who
19 are involved in transactions with the consumer in question. To retrieve the
20 information, merchants can click a button entitled “View customer data” in the
21 Shopify user interface, and Shopify will email this data to them.

22 **B. Shopify Discloses and Sells Consumers’ Sensitive Information to**
23 **Merchants, and Uses it to Assess Transaction Risk.**

24 Because over one million websites and other merchants use Shopify to sell
25 their products, Shopify has amassed an incredible amount of sensitive data
26 regarding consumers. Shopify leverages this data to assess the risk associated with

particular consumers and their transactions. Shopify distills this information into a profile for each consumer and payment and makes a risk recommendation to the merchant based on the consumer's profile. Shopify then adjusts and reapplies that score for future payments. Payment transactions with unacceptable indicators can be blocked or reversed.

35. In addition, Shopify makes information in the user profiles available to its merchant customers. For example, Shopify merchants can view a variety of information regarding the consumer transactions:

The full analysis for an order lists all the indicators. These indicators are marked with green, red, or grey icons to help you highlight different behaviour types.

Indicators

- Characteristics of this order are similar to non-fraudulent orders observed in the past
- Card Verification Value (CVV) is correct
- Billing street address matches credit card's registered address
- Billing address ZIP or postal code matches the credit card's registered address
- There was 1 payment attempt
- Payment was made with 1 credit card
- Billing country matches the country from which the order was placed
- The IP address used to place the order isn't a high risk internet connection (web proxy)
- Location of IP address used to place the order is Ottawa, Ontario, Canada
- Shipping address is 520 km from location of IP address

Green indicators show information about the order that is usually seen on legitimate orders. Red indicators show information about the order that is usually seen on fraudulent orders. Grey indicators give you additional information about the order that could be useful.

Figure 5: Shopify Analysis Indicators

1 36. At no time are consumers informed that Shopify is collecting and using
2 their sensitive payment information.

3 37. In fact, Shopify enables its merchant customers to set filters that can
4 preemptively block orders based on the information that Shopify collects on
5 consumers. Through the filters, Shopify's merchant customers can set rules that
6 can ban IP addresses, prevent certain customers from placing orders, and
7 automatically cancel orders that have "high" risk scores, among other things.
8 When a filter preemptively cancels an order, the consumer has no idea. Rather,
9 from the consumer's perspective, the order processes normally. But, in reality, the
10 order is "accepted" and then immediately canceled. Consumers will only see that
11 their credit card was declined, which can negatively impact the "score" that
12 Shopify assigns to the consumer and lead to future cancellations.

13 38. In addition to compiling risk profiles for each consumer, Shopify also
14 shares the information that it collects on consumers with third-parties, who, in
15 turn, use the consumers' data for their own purposes and share it with others. For
16 example, Shopify partners with Stripe, Inc. to handle payment processing. When a
17 consumer fills out a payment form, Shopify collects information regarding the
18 transaction and consumer. Shopify then shares that information with Stripe, which
19 enables Stripe to process the payment. Like Shopify, Stripe is also in the business
20 of developing individualized risk profiles on consumers. Stripe's "risk insights"
21 profiles for consumers, which includes sensitive information, such as (i) the
22 number of declined cards previously associated with an email address, (ii) the
23 time since the first card decline occurred, (iii) the IP address, and (iv) the credit
24 card number. Upon information and belief, Stripe uses the data that Shopify
25
26

1 shares with Stripe to process payments to build out its own risk profiles on
2 consumers, which it then markets and disseminates to its own customers.

3 39. Shopify also shares consumers' information with MaxMind in order to
4 create consumer risk profiles. When a user purchases an item through one of
5 Shopify's merchant customers, Shopify provides MaxMind with the consumers'
6 personal information and data regarding the transaction. MaxMind uses that
7 information to assign a risk score to the consumer and transaction, which Shopify,
8 in turn, shares with its merchant customers to evaluate the transaction and future
9 transactions. MaxMind markets and disseminates the consumer risk profiles to its
10 own customers.

11 40. Because Shopify conceals its involvement with consumer transactions,
12 consumers are unaware that Shopify shares their sensitive information with third
13 parties and are deprived of any ability to opt out of the dissemination of their data
14 from Shopify and the third-parties that are also receiving their sensitive data.

15 41. Shopify's collection, storage and dissemination of users' sensitive
16 information opens consumers to the possibility of identity theft, credit card theft,
17 and fraud, by storing their information, without their knowledge or consent,
18 creating a new venue that is open to vulnerabilities, such as hackers and phishing
19 scams. However, consumers who do not even know that their information is
20 collected and stored by Shopify or shared by Shopify with other third parties and
21 thus will not know to be weary of scams, and are deprived of the knowledge
22 necessary to protect their data.

23 42. The potential for identity theft, credit card theft and fraud of data
24 secretly collected and stored by Shopify is more than a mere possibility. From
25 2019-2020, certain Shopify staff members took advantage of the consumer data
26

1 Shopify unlawfully collected and stored. Shopify announced in September 2020
2 that it became aware of an incident in which data from about 200 merchants was
3 stolen.³ These staff members acquired information regarding consumer
4 transaction on Shopify's platform. The data included consumer names, e-mails,
5 addresses, and order details, including products, services purchased, payment
6 methods, and the last four digits of their credit cards.⁴ The staff members later
7 sold the data to others on the black market. It has been estimated that the data
8 breach involved the data of about 272,000 individuals. The consumer data that is
9 now in the hands of criminals was data that Shopify was never authorized to
10 collect at the outset. Because Shopify concealed its involvement with the
11 transactions, Shopify deprived consumers of the right to opt out of its collection
12 of their private information and, in doing so, has exposed consumers to the risk,
13 and for some consumers, the reality of identity theft, credit card theft and fraud.

14 **C. Shopify Does Not Inform Consumers About Its Activities.**

15 43. Shopify makes no effort to inform consumers regarding *any* of its
16 activities with respect to its interception and collection of consumer information
17 using merchant websites. Specifically, it does not inform consumers that:
18 (i) Shopify will intercept communications that consumers believe are being sent
19 exclusively to merchants; (ii) its software code is causing their devices to connect
20 to Shopify's computer servers; (iii) Shopify is placing tracking cookies on
21 consumers' computers; (iv) its software code is rendering the payment forms that
22 are displayed to consumers; (v) the sensitive information in the payment forms
23

24 _____
25 ³ See <https://community.shopify.com/c/Shopify-Discussion/Incident-Update/td-p/888971> (last accessed August 2, 2021).

26 ⁴ See <https://www.documentcloud.org/documents/20580321-us-grand-jury-indictment-tassilo-heinrich> (last accessed August 2, 2021).

1 will be sent to Shopify; (vi) sensitive information not expressly input by the
2 consumer—such as IP address, operating system, geolocation data, and item(s)
3 purchased—will also be collected from the consumer by Shopify; (vii) Shopify
4 will indefinitely store that sensitive information; (viii) Shopify will use
5 consumers’ information to assign risk scores to consumers, which could
6 subsequently be communicated to other merchants and used to deny consumers’
7 future payment attempts; (ix) Shopify will track consumers’ behavior across over
8 one million websites; (x) Shopify will make consumers’ sensitive information
9 available to any of its millions of customers who will accept payment—or who
10 have already accepted payment—from those consumers; and (xi) Shopify will
11 share consumer data with third-parties, such as Stripe, Inc. and MaxMind, Inc.

12 44. Shopify deliberately chose to hide its involvement from consumers.
13 Shopify did so to increase its profits, because it (i) understands that consumers
14 value the privacy of their communications and do not wish those communications
15 to be intercepted; (ii) understands that consumers do not wish for their activities
16 to be tracked across a vast network of third party merchants; and (iii) wants to
17 maximize the ability of its merchant customers to “white-label” payment forms, to
18 make it appear to consumers that the merchants have the sophistication to handle
19 payments themselves and without extensive third party involvement.

20 45. Although Shopify provides a default template for merchant websites
21 that includes, in the footer, a “powered with Shopify” link leading to Shopify’s
22 homepage, Shopify does not require merchants to use that template, or the link.
23 Indeed, Shopify provides instructions—including a dedicated video—to
24 merchants regarding how to remove the link. (See
25 <https://help.shopify.com/en/manual/online-store/themes/os/customize/remove->
26

1 powered-by-shopify-message (last accessed August 9, 2021).) As Shopify knows,
2 the vast majority—if not all—of its large merchants delete the link.

3 46. On information and belief, Shopify does not review its customers’
4 websites or mobile applications to determine whether its customers have disclosed
5 to consumers any of Shopify’s activities with respect to their personal
6 information.

7 47. Consumers visiting Shopify merchants’ webpages are not required to
8 view (through a link or otherwise), let alone agree to, Shopify’s Terms of Service
9 or Privacy Policy. Plaintiff has never agreed to any such policy.

10 48. As described above, the information that Shopify obtains from
11 consumers who purchase products from merchants utilizing the Shopify payment
12 forms includes consumers’ telephone numbers. Shopify maintains a database of
13 these consumer telephone numbers on its computers. Shopify then transmits, or
14 causes to be transmitted by a third party, marketing text messages to selected
15 telephone numbers from Shopify’s database. For example, Shopify sends
16 “abandoned cart” text messages to consumers that add items to their cart but do
17 not complete the checkout process. The telephone numbers messaged by Shopify
18 are assigned to cellular telephone service for which Plaintiff and Class members
19 incur charges for incoming messages.

20 **D. Plaintiff’s Experience**

21 49. Plaintiff purchased fitness apparel for his wife from IABMFG on or
22 about June 14, 2019. To do so, he used his iPhone’s Safari browser to establish a
23 secure, encrypted connection to IABMFG at <https://www.iambecoming.com>.

24 50. After adding products to his virtual shopping cart, Plaintiff was
25 presented with a checkout screen substantially similar to the screen shown at
26

1 Figure 1, *supra*. Plaintiff believed that all aspects of the checkout screen were
2 being generated by IABMFG, and sent over his browser's encrypted connection
3 with IABMFG.

4 51. Plaintiff was required to provide his private information in order to
5 complete the checkout process, including information such as his full name,
6 delivery address, billing address, phone number, and credit card number,
7 expiration date, and CVV code. Plaintiff provided this information, and then
8 clicked on the "Pay now" button to submit it. Plaintiff did not provide consent to
9 Shopify to send him text messages. Plaintiff did not provide consent for Shopify
10 to obtain, use, store, or share his sensitive information. When Plaintiff clicked the
11 "Pay now" button, he believed that his information would be sent directly to
12 IABMFG, through the secure, encrypted connection that his smartphone browser
13 had established with IABMFG.

14 52. Although Plaintiff was not aware of it, the IABMFG checkout page he
15 visited contained a link to the Shopify software code, which caused his
16 smartphone browser to load and execute the code. Although it was not disclosed
17 to Plaintiff, this code (i) enabled Shopify to intercept communications—including
18 those with his private information—that he reasonably believed would be sent
19 exclusively to IABMFG; (ii) enabled Shopify to install and/or confirm the
20 installation of a tracking cookie, containing a unique tracking code, on his
21 smartphone; (iii) caused his phone browser to establish a connection with
22 Shopify's computer network; and (iv) generated the payment form input elements
23 requiring Plaintiff to enter his private information. When Plaintiff submitted the
24 form containing his private information to complete the checkout process, his
25 private information was sent to Shopify's computer network, where it was stored,
26

1 analyzed, and processed. Plaintiff was never informed of any of these facts.
2 Indeed, Plaintiff did not know that Shopify was involved in the transaction at all,
3 because it was never disclosed to him.

4 53. Shopify has used Plaintiff's private information to assign a score to his
5 subsequent transactions with any other merchant that uses the Shopify network.
6 Shopify has offered to make and/or actually made Plaintiff's private information
7 available to any of its merchant customers who process payments made by
8 Plaintiff. Shopify has shared Plaintiff's private information with third parties,
9 such as Stripe Inc., and MaxMind, Inc. Shopify also used the private information
10 collected from Plaintiff to send him unsolicited marketing text messages about
11 IABMFG's products.

12 54. Had Plaintiff known that Shopify would install a tracking cookie on his
13 smartphone browser, for the purpose of tracking him across potentially hundreds
14 of thousands, if not millions, of websites, Plaintiff would not have purchased
15 products from IABMFG.

16 55. Had Plaintiff known that Shopify would collect, store, and analyze his
17 private information to increase its own profits, Plaintiff would not have purchased
18 products from IABMFG.

19 56. Had Plaintiff known that Shopify would offer to make his private
20 information to any of its millions of merchant customers with whom he may
21 engage in a subsequent financial transaction, Plaintiff would not have purchased
22 products from IABMFG.

23 57. Had Plaintiff known that Shopify would use his private information to
24 create a risk profile on him based on his subsequent transactions, Plaintiff would
25 not have purchased products from IABMFG.
26

Class Allegations

58. In addition to his individual claims, Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure.

59. Plaintiff brings this class action lawsuit on behalf of a proposed class of similarly situated persons, pursuant to Rule 23(b)(2) and (b)(3) of the Federal Rules of Civil Procedure, defined as follows:

The Class: All natural persons who, between August 13, 2017 and the present, submitted payment information via Shopify's software while located in California.

60. This action has been brought and may properly be maintained as a class action against Shopify because there is a well-defined community of interest in the litigation and the proposed class is easily ascertainable.

61. Numerosity: Plaintiff does not know the exact size of the Class, but he estimates that the Class is composed of more than 5,000 persons. The persons in the Class are so numerous that the joinder of all such persons is impracticable and the disposition of their claims in a class action rather than in individual actions will benefit the parties and the courts.

62. Common Questions Predominate: This action involves common questions of law and fact to the potential Class because each class member's claim derives from the same unlawful practices of Shopify. The common questions of law and fact predominate over individual questions, as proof of a common or single set of facts will establish the right of each member of the Class to recover. The questions of law and fact common to the Class include, but are not limited to, whether Shopify has violated Sections 631 and 635 of the California Invasion of Privacy Act; whether Shopify invaded the Class members' privacy rights in violation of the California Constitution; whether Shopify violated the

1 California Computer Data Access and Fraud Act; whether Shopify violated
2 California's Unfair Competition Law; and whether the Class members are entitled
3 to actual damages, statutory damages, and/or equitable relief for these violations.

4 63. Typicality: Plaintiff's claims are typical of the claims of other Class
5 members because, among other things, all such claims arise out of the same
6 unlawful course of conduct in which Shopify engaged. Plaintiff and those
7 similarly situated used Shopify payment forms and had their electronic
8 communications intercepted and disclosed to Shopify through the use of
9 Shopify's wiretaps.

10 64. Adequacy of Representation: Plaintiff will fairly and adequately protect
11 the interests of all class members because it is in his best interests to prosecute the
12 claims alleged herein to obtain full compensation due to him for the unfair and
13 illegal conduct of which he complains. Plaintiff also has no interests that are in
14 conflict with, or antagonistic to, the interests of Class members. Plaintiff has
15 retained highly competent and experienced class action attorneys to represent his
16 interests and those of the Class. By prevailing on his own claims, Plaintiff will
17 establish Shopify's liability to all Class members. Plaintiff and his counsel have
18 the necessary financial resources to adequately and vigorously litigate this class
19 action, and Plaintiff and counsel are aware of their fiduciary responsibilities to the
20 class members and are determined to diligently discharge those duties by
21 vigorously seeking the maximum possible recovery for class members.

22 65. Superiority: There is no plain, speedy, or adequate remedy other than
23 by maintenance of this class action. The prosecution of individual remedies by
24 members of the class will tend to establish inconsistent standards of conduct for
25 Shopify and result in the impairment of class members' rights and the disposition
26

1 of their interests through actions to which they were not parties. Class action
 2 treatment will permit a large number of similarly situated persons to prosecute
 3 their common claims in a single forum simultaneously, efficiently, and without
 4 the unnecessary duplication of effort and expense that numerous individual
 5 actions would engender. Furthermore, as the damages suffered by each individual
 6 member of the class may be relatively small, the expenses and burden of
 7 individual litigation would make it difficult or impossible for individual members
 8 of the class to redress the wrongs done to them, while an important public interest
 9 will be served by addressing the matter as a class action.

10 66. Plaintiff is unaware of any difficulties that are likely to be encountered
 11 in the management of this action that would preclude its maintenance as a class
 12 action.

13 CAUSES OF ACTION

14 First Cause of Action

15 **Violation of the California Invasion of Privacy Act, 16 California Penal Code § 631 17 (On Behalf of Plaintiff and the Class)**

18 67. Plaintiff realleges and incorporates by reference all paragraphs alleged
 19 herein.

20 68. The California Invasion of Privacy Act, codified at Cal. Penal Code §§
 21 630 to 638 (“CIPA”), includes the following statement of purpose:

22 The Legislature hereby declares that advances in science
 23 and technology have led to the development of new devices
 24 and techniques for the purpose of eavesdropping upon
 25 private communications and that the invasion of privacy
 26 resulting from the continual and increasing use of such
 devices and techniques has created a serious threat to the
 free exercise of personal liberties and cannot be tolerated in
 a free and civilized society.

1 69. To establish liability under section 631(a), a plaintiff need only
 2 establish that a defendant, “by means of any machine, instrument, contrivance, or
 3 in any other manner,” did any of the following:

4 Intentionally taps, or makes any unauthorized connection,
 5 whether physically, electrically, acoustically, inductively or
 6 otherwise, with any telegraph or telephone wire, line, cable,
 7 or instrument, including the wire, line, cable, or instrument
 8 of any internal telephonic communication system,

9 *Or*

10 Willfully and without the consent of all parties to the
 11 communication, or in any unauthorized manner, reads or
 12 attempts to read or learn the contents or meaning of any
 13 message, report, or communication while the same is in
 14 transit or passing over any wire, line or cable or is being
 15 sent from or received at any place within this state,

16 *Or*

17 Uses, or attempts to use, in any manner, or for any purpose,
 18 or to communicate in any way, any information so
 19 obtained,

20 *Or*

21 Aids, agrees with, employs, or conspires with any person or
 22 persons to unlawfully do, or permit, or cause to be done
 23 any of the acts or things mentioned above in this section.

24 (Cal. Penal Code § 631(a).)

25 70. Section 631(a) is not limited to phone lines, but also applies to “new
 26 technologies” such as computers, the Internet, and email. *See Matera v. Google*
Inc., 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to “new
 technologies” and must be construed broadly to effectuate its remedial purpose of
 protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D.
 Cal. Dec. 22, 2006) (CIPA governs “electronic communications”); *In re*
Facebook, Inc. Internet Tracking Litigation, 956 F.3d 589 (9th Cir. 2020)
 (reversing dismissal of CIPA and common law privacy claims based on
 Facebook’s collection of consumers’ Internet browsing history).

1 71. The following items constitute “machine[s], instrument[s], or
 2 contrivance[s]” under the CIPA (and even if they do not, Shopify’s deliberate and
 3 purposeful scheme that facilitated its interceptions falls under the broad statutory
 4 catch-all category of “any other manner”): (i) Shopify’s software code modules
 5 that are designed to intercept, collect, transmit, and track consumers’ private
 6 information; (ii) the Shopify computer servers, including the software code
 7 modules installed on those servers used to intercept, receive, transmit, read, track,
 8 analyze, and sell such private information; and (iii) the plan Shopify carried out to
 9 intercept, collect, transmit, read, track, analyze, and sell the Class members’
 10 private information, even though they had not consented (collectively, (i), (ii), and
 11 (iii) are referred to hereinafter as the “Shopify Instruments”).

12 72. The private information that was intercepted, collected, transmitted,
 13 received, tracked, and analyzed by the Shopify Instruments included at least the
 14 following information regarding each consumer:

- 15 • full name;
- 16 • home and/or delivery address;
- 17 • billing address;
- 18 • telephone number;
- 19 • email address;
- 20 • credit and/or debit card number, expiration date, and CVV number;
- 21 • internet IP addresses;
- 22 • the item(s) purchased from the merchant;
- 23 • the brand and model of the consumer’s computers or electronic devices;
- 24 • the identities of the consumer’s browsers;
- 25 • the operating systems that the consumer’s devices were using;
- 26

- the unique tracking codes, which enable Shopify to identify a particular consumer and track his or her activities across its entire merchant network, enabling Shopify to gather even more sensitive data about the consumer including, without limitation, (i) the number of declined cards that the consumer has used with Shopify merchants; (ii) how long ago one of the consumer's cards was last declined; (iii) whether the consumer had ever disputed a previous Shopify charge; (iv) whether any previous early fraud warnings were associated with the consumer; (v) the percentage of transactions that were authorized for the consumer over time; and (vi) the cards and other payment methods associated with the consumer's IP address.

(collectively, the information listed in the bullet points above shall be referred to as "Private Information.")

73. Specifically, the code caused the Private Information that the consumer intended to send to the merchant to instead be intercepted by the Shopify Instruments while in transit to the merchant. The merchant does not receive the Private Information and share it with Shopify, but instead it goes directly to Shopify.

74. Shopify never had authorization or consent from the consumers to intercept and collect the Private Information.

75. By enabling the Shopify Instruments to intercept, collect, transmit, receive, track, and analyze consumers' Private Information without their consent, and by communicating and selling that Private Information to Shopify merchants, Shopify violated Section 631(a) of the Privacy Act. In particular, Shopify:

- 1 • intentionally tapped, electrically or otherwise, the lines and/or instruments
- 2 of internet communication being used by Class members to access
- 3 merchant websites;
- 4 • intentionally made unauthorized connections, electrically or otherwise,
- 5 with the lines and/or instruments of internet communication being used by
- 6 Class members to access merchant websites;
- 7 • willfully, and without the consent of Class members, read and learned the
- 8 contents and/or meaning of their messages and communications
- 9 containing private information, while the same was in transit or passing
- 10 over lines of internet communication, or was being sent from and received
- 11 at locations in California;
- 12 • used Class members' Private Information to increase Shopify's profits;
- 13 • communicated and/or sold Class members' Private Information to
- 14 Shopify's merchant customers;
- 15 • communicated and/or sold Class members' Private Information to third
- 16 parties, such as Stripe and MaxMind; and
- 17 • aided, agreed with, and conspired with other persons (including, without
- 18 limitation, IABMFG, Stripe, and MaxMind) to unlawfully do, permit, and
- 19 cause to be done the above-listed activities.

20 76. The Class members have suffered loss by reason of these violations,
21 including, but not limited to, (i) violation of their right to privacy; (ii) loss of
22 value in their Private Information; and (iii) the price premium they were
23 unknowingly charged by IABMFG to compensate for Shopify's fees, since they
24 would not have entered into such financial transactions had they known their
25 Private Information would be intercepted, collected, shared and used.
26

1 77. The violation of section 631(a) constitutes an invasion of privacy
2 sufficient to confer Article III standing.

3 78. Unless enjoined, Shopify will continue to commit the illegal acts
4 alleged here. The Class Members continue to be at risk because they frequently
5 use the internet to search for information about products and services. They
6 continue to desire to use the internet for that purpose, including for the purpose of
7 shopping for various products and services. Shopify has intentionally designed its
8 payment forms to omit reference to Shopify, and to appear as though Shopify is
9 not involved in the transaction. Accordingly, the Class Members have no practical
10 way to know if their website communications will be monitored or recorded by
11 Shopify and/or if Shopify will collect further Private Information from them.
12 Further, Shopify has already collected their Private Information, and is currently
13 sharing, and will continue sharing, that information with its other merchant
14 customers and third parties, unless and until enjoined by this Court.

15 79. The Class Members seek all relief available under Cal. Penal Code §
16 637.2, including injunctive relief and statutory damages of \$5,000 per violation.

17 **Second Cause of Action**

18 **Violation of the California Invasion of Privacy Act, 19 California Penal Code § 635 20 (On Behalf of Plaintiff and the Class)**

21 80. Plaintiff realleges and incorporates by reference all paragraphs alleged
22 herein.

23 81. California Penal Code § 635 provides as follows:

24 Every person who manufactures, assembles, sells, offers for
25 sale, advertises for sale, possesses, transports, imports, or
26 furnishes to another any device which is primarily or
 exclusively designed or intended for eavesdropping upon
 the communication of another, or any device which is

1 primarily or exclusively designed or intended for the
2 unauthorized interception or reception of communications
3 between cellular radio telephones or between a cellular
4 radio telephone and a landline telephone in violation of
5 Section 632.5, or communications between cordless
6 telephones or between a cordless telephone and a landline
7 telephone in violation of Section 632.6 , shall be punished
8 by a fine not exceeding two thousand five hundred dollars.

9 82. Shopify intentionally manufactured, assembled, sold, offered for sale,
10 advertised for sale, possessed, transported, imported, and/or furnished one or
11 more wiretap devices (i.e., the Shopify Instruments, including the software code
12 modules therein) primarily or exclusively designed or intended for eavesdropping
13 upon the communication of another.

14 83. In particular, the Shopify Instruments contain software code modules
15 that are primarily or exclusively designed to intercept, collect, transmit, receive,
16 and track communications that Class members reasonably (but erroneously)
17 believed would be sent directly and exclusively to the merchant. Further, although
18 the Class members intended to provide only information necessary for the
19 purchase of products and services, and to provide that information directly and
20 exclusively to the merchant, the software code modules of the Shopify
21 Instruments were designed to (and in fact did) intercept, collect, transmit, receive,
22 track, analyze, and sell the Private Information of the Class members.

23 84. The Class members did not consent to any of Shopify's actions in
24 implementing its wiretaps.

25 85. The Class members have suffered loss by reason of these violations,
26 including, but not limited to, (i) violation of their right to privacy; (ii) loss of
value in their Private Information; and (iii) the price premium they were
unknowingly charged by IABMFG to compensate for Shopify's fees, since they

1 would not have entered into such financial transactions had they known their
2 Private Information would be intercepted, collected, shared and used.

3 86. The violation of section 635 constitutes an invasion of privacy
4 sufficient to confer Article III standing.

5 87. Unless enjoined, Shopify will continue to commit the illegal acts
6 alleged here. The Class members continue to be at risk because they frequently
7 use the internet to search for information about products and services. They
8 continue to desire to use the internet for that purpose, including for the purpose of
9 shopping for various products and services. Defendant Shopify has intentionally
10 designed Shopify's payment forms to omit reference to Shopify, and to appear as
11 though Shopify is not involved in the transaction. Accordingly, the Class
12 Members have no practical way to know if their website communications will be
13 monitored or recorded by Shopify and/or if Shopify will collect further Private
14 Information from them. Further, Shopify has already collected their Private
15 Information, and is currently sharing, and will continue sharing, that information
16 with its other merchant customers and/or third parties, unless and until enjoined
17 by this Court.

18 88. The Class members seek all relief available under Cal. Penal Code §
19 637.2, including injunctive relief and statutory damages of \$5,000 per violation.

20 **Third Cause of Action**

21 **Invasion of Privacy Under California's Constitution**
22 **(On Behalf of Plaintiff and the Class)**

23 89. Plaintiff realleges and incorporates the paragraphs of this Class Action
24 Complaint as if set forth herein.

25 90. California's constitution creates a right to privacy, and further creates a
26 right of action against private entities such as Shopify.

1 91. The principal purpose of this constitutional right is to protect against
2 unnecessary information gathering, use, and dissemination by public and private
3 entities, including Shopify.

4 92. To plead a California constitutional privacy claim, a plaintiff must
5 show an invasion of (i) a legally protected privacy interest; (ii) where the plaintiff
6 had a reasonable expectation of privacy in the circumstances; and (iii) conduct by
7 the defendant constituting a serious invasion of privacy.

8 93. Shopify has intruded upon the following legally protected privacy
9 interests of the Class members: (i) the California Wiretap Act as alleged above;
10 (ii) the California Constitution, which guarantees Californians the right to
11 privacy; and (iii) a Fourth Amendment right to privacy.

12 94. The Class members had a reasonable expectation of privacy. They
13 directed their electronic devices to access merchant websites, such as IABMFG,
14 and to form an encrypted connection with those websites, such as
15 <https://www.iambecoming.com>. When they were presented with the payment
16 form on merchants' websites, such as IABMFG's, they reasonably expected that
17 their Private Information would be sent, in encrypted form, to the merchant, such
18 as IABMFG. They reasonably expected that no third party, such as Shopify,
19 would intercept and obtain the Private Information they submitted using the
20 forms. They further reasonably expected that no third party, such as Shopify,
21 would obtain Private Information about them that was not included on the form,
22 such as their IP addresses, device identities, and operating systems. The Class
23 members further reasonably expected that no one would store and assemble their
24 information, make profiles about them, and then make those profiles and Private
25 Information available to other merchants, as Shopify routinely does. The Class
26

1 members further reasonably expected that their Private Information would not be
2 shared with other unknown third parties, such as Stripe and MaxMind.

3 95. Shopify's actions constituted a serious invasion of privacy in that it
4 invaded a zone of privacy protected by the Fourth Amendment (i.e., one's
5 personal communications), and violated criminal laws on wiretapping and
6 invasion of privacy. These acts constitute an egregious breach of social norms that
7 is highly offensive.

8 96. Shopify's intentional intrusion into the Class members' privacy was
9 also highly offensive to a reasonable person in that Shopify violated criminal and
10 civil laws designed to protect individual privacy and against theft. Shopify also
11 disseminated Class members' financial and credit information.

12 97. Shopify lacked a legitimate business interest in enabling the Shopify
13 Instruments to intercept, collect, transmit, receive, track, analyze, and sell the
14 Private Information of the Class members without their consent.

15 98. The Class members have been damaged by Shopify's invasion of their
16 privacy and are entitled to just compensation and injunctive relief.

17 **Fourth Cause of Action**

18 **Intrusion Upon Seclusion**
19 **(On Behalf of Plaintiff and the Class)**

20 99. Plaintiff realleges and incorporates by reference all paragraphs alleged
21 herein.

22 100. A plaintiff asserting a claim for intrusion upon seclusion must plead
23 (i) that the defendant intentionally intruded into a place, conversation, or matter as
24 to which the plaintiff had a reasonable expectation of privacy; and (ii) that the
25 intrusion was highly offensive to a reasonable person.
26

1 101. By enabling the Shopify Instruments to intercept, collect, transmit,
2 receive, track, and analyze consumers' Private Information without their consent,
3 and by communicating and selling that Private Information to Shopify merchants
4 and other third parties, such as Stripe and MaxMind, Shopify intentionally
5 intruded upon the solitude or seclusion of the Class members, in that Shopify
6 effectively placed itself in the middle of communications to which it was not
7 invited, welcomed, or authorized.

8 102. The Class members did not consent to, authorize, or know about
9 Shopify's intrusion at the time it occurred. Further, they never agreed that Shopify
10 could install a tracking cookie on their devices to track them across the Shopify
11 merchant network, nor did they agree that Shopify could transmit, receive, track,
12 and analyze their private information, and disclose that information to other
13 merchants in the Shopify network and/or other third parties such as Stripe and
14 MaxMind.

15 103. Shopify's intentional intrusion on the Class members' solitude or
16 seclusion without consent would be highly offensive to a reasonable person. The
17 Class members reasonably expected, based on (i) the fact that they had
18 established a secure, encrypted connection to the IABMFG website; (ii) the fact
19 that no disclosure was made to them that Shopify was involved in the transaction
20 that their Private Information would be submitted exclusively to the merchant,
21 and would be used only for the purpose of making their purchase.

22 104. Shopify's intentional intrusion into the Class members' private
23 conversations was highly offensive to a reasonable person in that it violated state
24 laws designed to protect individual privacy.
25
26

1 105. The surreptitious taking and disclosure of personal, confidential, and
2 private information from the Class members was highly offensive because it
3 violated expectations of privacy that have been established by general social
4 norms. Privacy polls and studies consistently show that the overwhelming
5 majority of Americans believe one of the most important privacy rights is the
6 need for an individual's affirmative consent before personal data is harvested or
7 shared.

8 106. Shopify intentionally engages in the misconduct alleged herein to
9 generate substantial profit, not only through its transaction fees, but also by
10 improving the functionality of its products by creating consumer profiles, and by
11 selling consumers' Private Information to Shopify merchants and/or other third
12 parties.

13 107. As a result of Shopify's actions, the Class members have suffered harm
14 and injury, including but not limited to the invasion of their privacy rights.

15 108. Unwanted access to data by electronic or other covert means, in
16 violation of the law or social norms is actionable under California law.

17 109. The Class members have been damaged as a direct and proximate result
18 of Shopify's invasion of their privacy and are entitled to just compensation.

19 110. The Class members seek appropriate relief for that injury, including but
20 not limited to damages that will reasonably compensate them for the harm to their
21 privacy interests as well as disgorgement of profits made by Shopify as a result of
22 its intrusions upon the Class members' privacy.

23
24 **Fifth Cause of Action**

25 **Violation of the California Computer Data Access and Fraud Act,**
26 **Cal. Penal Code § 502**
 (On Behalf of Plaintiff and the Class)

1
2 111. Plaintiff realleges and incorporates by reference all paragraphs alleged
3 herein.

4 112. Cal. Penal Code § 502 provides that any person who commits any of
5 the following acts is guilty of a public offense:
6

7 (1) Knowingly accesses and without permission alters, damages, deletes,
8 destroys, or otherwise uses any data, computer, computer system, or
9 computer network in order to either (A) devise or execute any scheme or
artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain
money, property, or data.

10 (2) Knowingly accesses and without permission takes, copies, or makes use
11 of any data from a computer, computer system, or computer network, or takes
12 or copies any supporting documentation, whether existing or residing internal
or external to a computer, computer system, or computer network.

13 113. Smartphone devices with the capability of using mobile apps are
14 “computers” within the meaning of the statute.

15 114. Shopify violated the Cal. Penal Code § 502(c)(1) and (2) by knowingly
16 accessing Plaintiff’s and the Class member’s data by surreptitiously and
17 intentionally installing software code and cookies onto their devices, including
18 Plaintiff’s iPhone. The software code and cookies enabled Shopify to take, copy,
19 or make use of Plaintiff’s and the Class members’ Private Information and data
20 from their transactions across Shopify’s merchant network, as described above.

21 115. Shopify took, copied, or made use of Plaintiff’s and the Class
22 members’ data and Private Information, even though Plaintiff and the Class
23 members never gave Shopify permission to do so. Because Shopify intentionally
24 designs the websites that it hosts on behalf of its merchant-customers and its
25 payment forms to omit its involvement with the transaction, users, such as
26

1 Plaintiff and the Class members, have no idea that Shopify is taking, copying or
2 using their data. Further, Shopify failed to disclose its Privacy Policy or Terms of
3 Use to Plaintiff and the Class members in the course of their transactions with
4 Shopify's merchant customers and, therefore, Plaintiff and the Class members
5 never consented to allow Shopify to take, copy or use their data. In doing so,
6 Shopify wrongfully obtained control of Plaintiff's and the Class members' data
7 and now uses that data to generate individualized profiles on users that Shopify
8 markets to its merchant customers, and provide Plaintiff's and Class members'
9 data to third parties, such as Stripe and MaxMind, among other things.

10 116. The Class members have suffered loss by reason of these violations,
11 including, but not limited to, (i) violation of their right to privacy; (ii) loss of
12 value in their Private Information; and (iii) the price premium they were
13 unknowingly charged by IABMFG to compensate for Shopify's fees, since they
14 would not have purchased the products had they known their data was being
15 accessed, copied, taken, obtained and used without permission.

16 117. The Class members seek all relief available under Cal. Penal Code §
17 502(e), including compensatory damages and/or disgorgement of profits made by
18 Shopify and injunctive or other equitable relief.

19 118. Plaintiff and the Class members further seek punitive or exemplary
20 damages pursuant to Cal. Penal Code § 502(e)(4) because Shopify's conduct was
21 willful and oppressive, fraudulent, and/or malicious as defined in Cal. Civil Code
22 § 3294.

23 119. Plaintiff and the Class members also seek their reasonable attorney's
24 fees pursuant to Cal. Penal Code § 502(e)(2).
25
26

Sixth Cause of Action

**Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, et seq.
(On Behalf of Plaintiff and the Class)**

120. Plaintiff realleges and incorporates by reference all paragraphs alleged herein.

121. Shopify is a “person” under Cal. Bus. & Prof. Code § 17201.

122. Shopify created and implemented a scheme to obtain the Private Information from the Class members through a pervasive pattern of false and misleading omissions. Shopify concealed and failed to disclose to the Class members the following facts: (i) that the Shopify payment forms were being provided by Shopify; (ii) that Shopify would intercept the communications, including the Private Information, that Class members reasonably believed would be sent directly and exclusively to the merchant; (iii) that Shopify would collect and store the Class members’ Private Information, including information entered by them in the forms, as well as other Private Information not expressly provided by them; (iv) that Shopify would access Class members’ data from their devices without authorization and install a tracking cooking on their devices and track their behavior across its entire merchant network; (v) that Shopify would sell and make that information available to its other customers and other third parties, such as Stripe and/or MaxMind, who, in turn, shared Class members’ data with their own customers; (vi) that Shopify would continue to monitor the status of the transactions with their banks, including whether and why they disputed the charges; or (vii) that Shopify would use the information to affect future financial transactions performed by the Class members. Indeed, Shopify concealed and

1 failed to disclose its identity to the Class members; it did not disclose that it was
2 involved in the transactions at all.

3 123. These omissions were misleading and deceptive.

4 124. Shopify's conduct was unfair and unconscionable, particularly because
5 Shopify intruded on communications that the Class members reasonably believed
6 to be private, and also because Shopify made and/or offered to make their Private
7 Information available to any of its merchant customers and third parties who, at
8 any time in the past or future, were involved in a financial transaction with the
9 Class members. Unbeknownst to the Class members and without their consent,
10 the third parties with whom Shopify shared Class members' data, including Stripe
11 and MaxMind, in turn shared Class members' data with their own customers.

12 125. Shopify's conduct was fraudulent and deceptive because the omissions
13 at issue were likely to, and in fact did, deceive reasonable consumers, including
14 the Class members. Reasonable consumers, including the Class members, would
15 have found it material to their purchasing decisions that Shopify would intercept,
16 collect, transmit, receive, track, and analyze consumers' private information
17 without their consent, and share that Private Information with Shopify merchants
18 and other third parties, such as Stripe and MaxMind, who, in turn, disseminate the
19 data to their own customers. Knowledge of these facts would have been a
20 substantial factor in the Class members' decisions to engage in the financial
21 transactions described herein.

22 126. Shopify owed the Class members a duty to disclose these facts because
23 they were exclusively known and/or accessible to Shopify, who had superior
24 knowledge of its activities with respect to the private information of the Class
25
26

1 members; because Shopify actively concealed the facts; and because Shopify
2 intended for consumers to rely on the omissions in question.

3 127. As set forth above, in engaging in financial transactions using Shopify
4 payment forms, the Class members relied on Shopify's omissions. Reasonable
5 consumers would have been expected to have relied on the omissions, particularly
6 because they had directed their browsers and/or mobile applications to visit and
7 establish secure connections to the merchant's website, and because they were not
8 informed that Shopify would intercept and receive their communications, which
9 they believed would be sent directly and exclusively to the merchant over the
10 secure connection with the merchant website.

11 128. Shopify's conduct was also unlawful in that it violated the following
12 statutes: the California Invasion of Privacy Act, Cal. Penal Code §§ 635 and 637;
13 the California Online Privacy Protection Act of 2003 ("CalOPPA"), Cal. Bus. &
14 Prof. Code § 22575 *et seq.*; the California Consumer Privacy Act of 2018
15 ("CCPA"), Cal. Bus. & Prof. Code § 1427 *et seq.*; and the California Computer
16 Data Access and Fraud Act, Cal. Penal Code § 502. Shopify's conduct was also
17 unlawful because it intruded upon Plaintiff's and the Class members' seclusion
18 and violated the California Constitution by invading Class members' privacy, as
19 described above.

20 129. Shopify was subject to CalOPPA because it is an entity that owns or
21 operates a commercial website or online service that collects and maintains
22 personally identifiable information, including California consumers' first and last
23 names, street address, email address, telephone number, who use or visit said
24 website or online service. Shopify violated CalOPPA because it does not
25 conspicuously post its privacy policy on websites it operates on behalf of its
26

1 merchant customers or websites in which Shopify performs online services. These
2 websites fail to include Shopify's privacy policy or a text or icon link to Shopify's
3 privacy policy on the merchant customers' homepages or first significant page
4 after entering the website.

5 130. Shopify also violated the CCPA because, among other things, it is a
6 business that controls the collection of consumers' personal information and fails
7 to make any of the disclosures required pursuant to Cal. Bus. & Prof. Code §
8 1798.100 at or before it collects consumers' personal information.

9 131. Shopify engaged in conduct that is unfair and unconscionable because
10 its activities with respect to Class members' Private Information offends public
11 policy, is immoral unethical, oppressive, outrageous, unscrupulous, and
12 substantially injurious, and has caused substantial harm that greatly outweighs
13 any possible utility from the conduct.

14 132. Shopify's conduct actually and proximately caused the Class members
15 to lose money or property. Absent Shopify's unlawful, unfair, and fraudulent
16 conduct, Plaintiff and Class Members would have behaved differently and would
17 not have entered into financial transactions with merchants such as IABMFG.
18 Further, Shopify's unlawful activities and use of the Class members' Private
19 Information enabled it to charge transaction fees to merchants, the price of which
20 the Class members covered through increased merchant fees.

21 133. The Class members seek—on behalf of themselves and each member
22 of the class—restitution, injunctive relief, and reasonable attorneys' fees, as well
23 as any other relief the Court may deem just or proper.

24
25 **PRAYER FOR RELIEF**

26 WHEREFORE, Plaintiff, on behalf of himself and those similarly situated,

respectfully requests that the Court enter judgment against Defendants as follows:

- A. Certification of the proposed Class, including appointment of Plaintiff's counsel as class counsel;
- B. An award of compensatory damages, including statutory damages where available, to Plaintiff and the Class Members against Defendants for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including both pre- and post-judgment interest thereon, except as to those causes of action where compensatory damages are not legally available;
- C. An order for full restitution;
- D. An order requiring Defendants to disgorge revenues and profits wrongfully obtained;
- E. An order temporarily and permanently enjoining Defendants from continuing the unlawful, deceptive, fraudulent, and unfair business practices alleged in this Complaint;
- F. For reasonable attorneys' fees and the costs of suit incurred; and
- G. For such further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury.

Dated: August 13, 2021

GUTRIDE SAFIER LLP

/s/ Seth A. Safier
 Seth A. Safier, Esq.
 Marie A. McCrary, Esq.
 Todd Kennedy, Esq.
 100 Pine Street, Suite 1250
 San Francisco, CA 94111